```
void OVERFLOW ( char *pointer) {

   char SMALL [100];

   strcpy SMALL,pointer);
}

void MAIN () {
   char LARGE [2000];
   int  i;

for (i=0 ; i<2000 ; i++)
   LARGE [i] = 'x' ;
   overflow (LARGE);
}
```

10

FIG. 1A

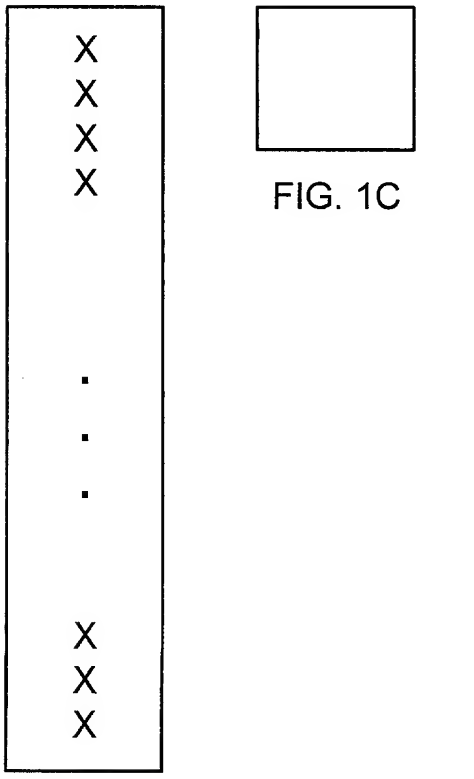

FIG. 1B

FIG. 1C

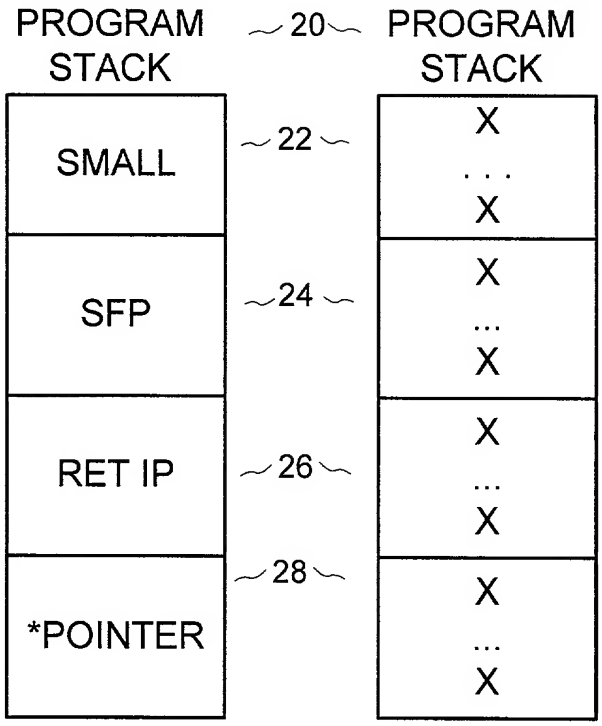

FIG. 1D

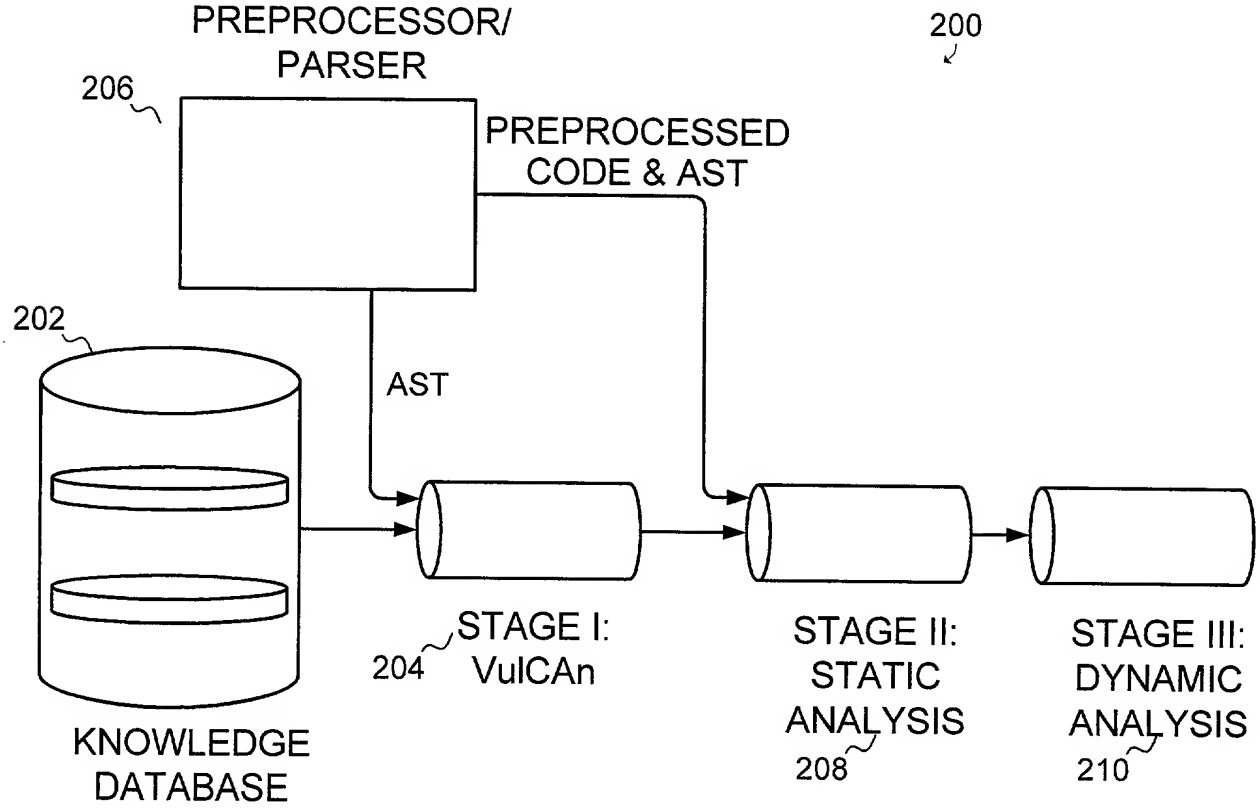
PREPROCESSOR/
PARSER
206
200
PREPROCESSED
CODE & AST
202
AST
STAGE I:
VulCAn
204
STAGE II:
STATIC
ANALYSIS
208
STAGE III:
DYNAMIC
ANALYSIS
210
KNOWLEDGE
DATABASE

FIG. 2

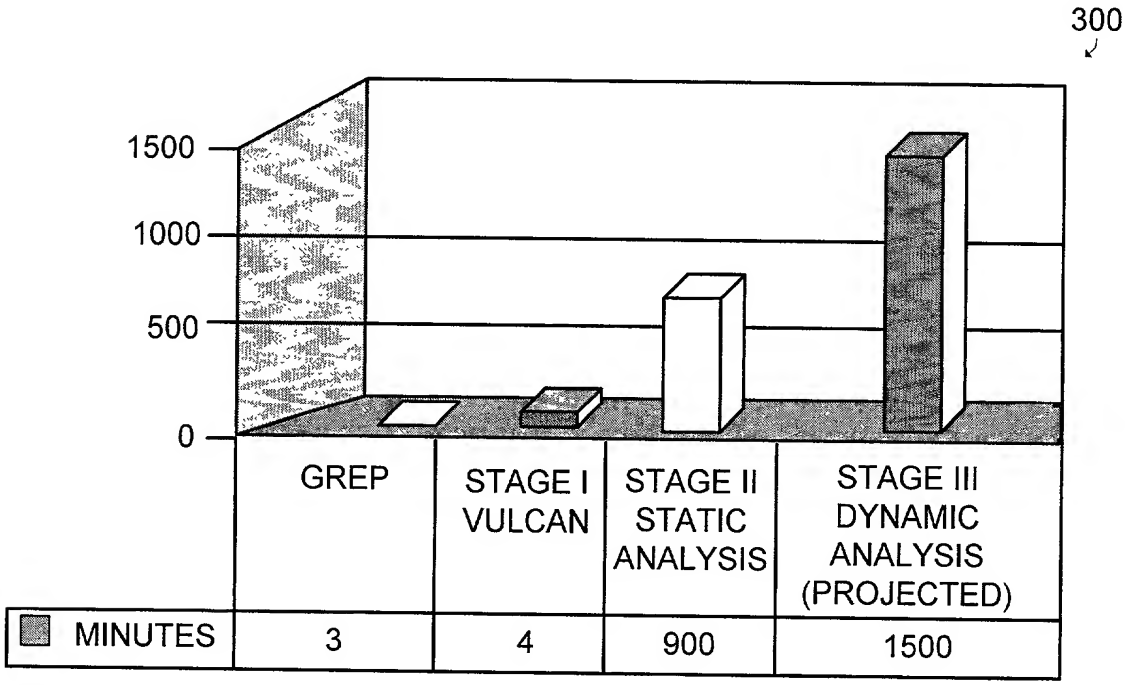
300
1500
1000
500
0
GREP
STAGE I
VULCAN
STAGE II
STATIC
ANALYSIS
STAGE III
DYNAMIC
ANALYSIS
(PROJECTED)
MINUTES
3
4
900
1500

FIG. 3